#4

Attorney Docket No.:04329.2151

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of

Hideo SHIMIZU et al

Serial No.: 09/379,791) Group Art Unit: 2766

Filed: August 24, 1999) Examiner: Not Assigned

For: DATA PROCESSOR, COMMUNICATION SYSTEM AND RECORDING MEDIUM

CLAIM FOR PRIORITY

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Under the provisions of 35 U.S.C. § 119, Applicants hereby claim the benefit of the filing date of Japanese Patent Application No. 10-237205, filed on August 24, 1998, for the above-identified U.S. patent application.

In support of Applicants' claim for priority, filed herewith is a certified copy of the above.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P.

By: _____
Richard V. Burgujian
Reg. No. 31,744

Dated: October 22, 1999
RVB/FPD/sci
Enclosure

LAW OFFICES
FINNEGAN, HENDERSON, FARABOW, GARRETT, & DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, D.C. 20005
202-408-4000

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９８年　８月２４日

出願番号
Application Number: 平成１０年特許願第２３７２０５号

出願人
Applicant (s): 株式会社東芝

１９９９年　８月１６日

特許庁長官
Commissioner,
Patent Office 伊佐山建志

出証番号　出証特平１１－３０５７５１４

【書類名】　特許願

【整理番号】　A009801804

【提出日】　平成10年 8月24日

【あて先】　特許庁長官　殿

【国際特許分類】　G06F 7/00

【発明の名称】　データ処理装置及び通信システム並びに記録媒体

【請求項の数】　9

【発明者】

【住所又は居所】　東京都府中市東芝町１番地　株式会社東芝府中工場内

【氏名】　清水　秀夫

【発明者】

【住所又は居所】　東京都府中市東芝町１番地　株式会社東芝府中工場内

【氏名】　佐野　文彦

【特許出願人】

【識別番号】　000003078

【氏名又は名称】　株式会社　東芝

【代理人】

【識別番号】　100058479

【弁理士】

【氏名又は名称】　鈴江　武彦

【電話番号】　03-3502-3181

【選任した代理人】

【識別番号】　100084618

【弁理士】

【氏名又は名称】　村松　貞男

【選任した代理人】

【識別番号】　100068814

【弁理士】

【氏名又は名称】　坪井　淳

【選任した代理人】

【識別番号】　100092196

【弁理士】

【氏名又は名称】　橋本　良郎

【選任した代理人】

【識別番号】　100091351

【弁理士】

【氏名又は名称】　河野　哲

【選任した代理人】

【識別番号】　100088683

【弁理士】

【氏名又は名称】　中村　誠

【選任した代理人】

【識別番号】　100070437

【弁理士】

【氏名又は名称】　河井　将次

【手数料の表示】

【予納台帳番号】　011567

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9705037

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　データ処理装置及び通信システム並びに記録媒体

【特許請求の範囲】

【請求項１】　暗号化用の鍵を用いて平文を暗号文に暗号化し、及び又は、復号用の鍵を用いて暗号文を平文に復号するデータ処理装置であって、

前記鍵の何れか若しくはその鍵変換結果に基づいて、鍵変換処理及び拡大鍵の出力を行うインボリューションな複数の鍵変換関数を順次接続してなるとともに、前記鍵変換処理の結果を前記鍵変換関数間で順次又は逆順に引き渡す鍵変換部と、

前記拡大鍵を用いて暗号化処理及び又は復号処理を行うインボリューションな複数のラウンド関数を順次接続してなるとともに、前記ラウンド関数での処理結果をラウンド関数間で順次又は逆順に引き渡す攪拌部と

を備えたことを特徴とするデータ処理装置。

【請求項２】　前記鍵変換関数は、第１の鍵又はその鍵変換結果を前記鍵変換処理の対象とするとともに、第２の鍵を用いて前記鍵変換処理を行うことを特徴とする請求項１記載のデータ処理装置。

【請求項３】　前記第２の鍵は、前記暗号化用の鍵、及び又は、前記復号用の鍵に含まれることを特徴とする請求項２記載のデータ処理装置。

【請求項４】　前記第２の鍵には複数の種類が設けられ、前記暗号化用の鍵、及び又は、前記復号用の鍵は、当該複数種類の第２の鍵を含むことを可能として可変長の鍵としたことを特徴とする請求項３記載のデータ処理装置。

【請求項５】　前記鍵変換関数は、前記攪拌部と同一のラウンド関数を含むことを特徴とする請求項１乃至４のうち、何れか一項記載のデータ処理装置。

【請求項６】　前記請求項１乃至５のうち、何れか一項記載のデータ処理装置を備えるとともに、前記暗号化用の鍵でありかつ前記復号用の鍵である一の鍵を保持する一の通信装置と、

前記請求項１乃至５のうち、何れか一項記載のデータ処理装置を備えるとともに、前記一の鍵を前記鍵変換部で鍵変換処理した結果である他の鍵を前記暗号化用の鍵でありかつ前記復号用の鍵として保持する他の通信装置と

を備えたことを特徴とする通信システム。

【請求項７】　暗号化用の鍵を用いて平文を暗号文に暗号化し、及び又は、復号用の鍵を用いて暗号文を平文に復号するデータ処理装置を制御するプログラムであって、

前記鍵の何れか若しくはその鍵変換結果に基づいて、鍵変換処理及び拡大鍵の出力を行うインボリューションな複数の鍵変換関数を順次接続してなるとともに、前記鍵変換処理の結果を前記鍵変換関数間で順次又は逆順に引き渡す鍵変換部と、

前記拡大鍵を用いて暗号化処理及び又は復号処理を行うインボリューションな複数のラウンド関数を順次接続してなるとともに、前記ラウンド関数での処理結果をラウンド関数間で順次又は逆順に引き渡す攪拌部として

コンピュータを機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項８】　前記鍵変換関数は、第１の鍵又はその鍵変換結果を前記鍵変換処理の対象とするとともに、第２の鍵を用いて前記鍵変換処理を行う請求項７記載の記録媒体。

【請求項９】　前記鍵変換関数は、前記攪拌部と同一のラウンド関数を含む請求項７又は８記載の記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明はデータ処理装置及び通信システム並びに記録媒体に関する。

【０００２】

【従来の技術】

近年の計算機・通信技術の発達により、データ通信時に送信データを暗号化することが一般的になっている。この暗号化の方式には公開鍵方式と秘密鍵方式とがあり、秘密鍵方式ではＤＥＳ方式が広く用いられている。

【０００３】

図８はＤＥＳ方式を説明する図である。

ＤＥＳ方式による暗号化では、図８（ａ）に示すように平文に初期転置ＩＰを施したデータに対し、ラウンド関数による処理を１６回施す。さらにラウンド関数処理されたデータに初期転置の逆転置IP^{-1}を施すことで暗号文を得ている。また、各ラウンド関数に対し、元の秘密鍵から生成される拡大鍵を与えることでラウンド関数における処理が実行される。

【０００４】

つまり、ＤＥＳ方式による暗号化装置は、多数のラウンド関数によって暗号化対象となるデータを攪拌する攪拌部と、攪拌部の各ラウンド関数に拡大鍵を与える鍵変換部をその主要構成としている。

【０００５】

一方、ＤＥＳ方式による復号は、図８（ｂ）に示すように、暗号化時とは逆の順番で復号対象のデータにラウンド関数の処理を施す。したがって、鍵変換部からの拡大鍵も、暗号化時の最後のラウンド関数で使用されたものから順番に生成する。

【０００６】

このＤＥＳ方式における第１の利点は、暗号化回路と復号回路のかなりの部分を共通化できるところにある。つまり、図８（ａ）、図８（ｂ）に示すように、攪拌部のラウンド関数は、暗号化時と復号時で使用する順番が逆になるだけで同一のものを使用できる。

【０００７】

ＤＥＳ方式の第２の利点は、同一の秘密鍵で暗号化と復号の双方を行うため、管理対象となる鍵が常に一つのみですむということである。ここで、ＤＥＳ方式では、唯一の鍵でもって、拡大鍵を逆順に生成できるようにするため、鍵変換部２では次のような処理を行っている。

【０００８】

すなわち暗号化処理の場合には、秘密鍵を左巡回シフト（左ローテート）することで各拡大鍵を作成する。このシフト量の合計値を一定値に定めることで拡大鍵の逆順生成を可能とする。すなわち復号時には秘密鍵を逆に右巡回シフト（右ローテート）して各拡大鍵を生成すればよい。これにより暗号化時の最後の拡大

鍵と復号時の最初の拡大鍵が同じものとなる。

【０００９】

【発明が解決しようとする課題】

しかしながら、上記したＤＥＳ方式には、次のような問題がある。

まず、鍵変換部での処理は、暗号化時は左巡回シフト、復号時は右巡回シフトと異なる処理を行っており、従って、暗号化装置及び復号装置において、この鍵変換部では同一の回路を使用できない。すなわち現実の装置として、データの暗号化又は復号を行う暗復号装置を作成する場合には、暗号化処理と復号処理とに共通して使用できる回路部分が必ずしも十分に多くない。したがって、全体の回路規模を十分に小さくすることができない。

【００１０】

次に、ＤＥＳでは鍵変換部の処理は転置処理のみで構成されるため、一般に弱鍵と呼ばれる安全性の弱い暗号鍵が存在するという安全性の問題がある。また、鍵変換部での処理は非線形でなく、ここで生成される拡大鍵の暗号強度への貢献はそれほど大きなものとはいえない。ＤＥＳにおいて非線形な部分は、図８（ｃ）に示すラウンド関数内の関数ｆにおけるＳボックスといわれる部分のみである。

【００１１】

したがって、鍵変換部から生成される拡大鍵が暗号強度に十分に貢献する暗号化手法が要望されている。

一方、ＤＥＳのもつ弱鍵のような鍵変換部の弱点を排除する試みとして、同変換部にハッシュ関数のような一方向性の関数を用いるという試みがある。例えばＦＥＡＬは一方向関数を使って鍵を変換することで攪拌部が必要とする拡大鍵を計算している。

【００１２】

ＦＥＡＬの方法は弱鍵が存在せずより安全な方法であるが、鍵変換部に一方向関数を用いたのではＤＥＳの場合のように逆順に拡大鍵を生成できない。そこで、この方法であっても復号を可能とするためには、暗号化に用いるのと同一の鍵変換部を用いて秘密鍵から一旦全ての拡大鍵を生成し、これをバッファに保存す

る。そして、バッファに格納された各拡大鍵を生成順と逆順に取り出して復号処理を行うのである。

【００１３】

しかしながら、このようにしたのではまず拡大鍵の格納に関わるコスト、つまり鍵格納のために必要なメモリ容量が増大するという問題がある。また、単に必要メモリ量が増えるというだけでなく、一時的とはいえ、多数の鍵を管理する必要が生じる。さらに、復号化にあたって事前に行われる鍵拡大処理のため、復号処理時間が長くなるという問題もある。

【００１４】

以上のように従来の技術では、拡大鍵を逆順に生成できるようにすると、秘密鍵暗号の装置規模を十分に小さくできず、また安全性が低くなる。一方、安全性を高めようとすると、拡大鍵を逆順に生成できなくなりメモリ資源を要するばかりか、一時的には多数の鍵を管理する必要が生じ、さらに処理時間が長くなるという問題があった。

【００１５】

本発明は、このような実情を考慮してなされたもので、秘密鍵暗号の装置規模を小さくすることを可能とし、かつ鍵の安全性を高めることができ、さらには鍵管理も容易なものとすることができるデータ処理装置及び通信システム並びに記録媒体を提供することを目的とする。

【００１６】

【課題を解決するための手段】

本発明の骨子は、変換と逆変換が同一となるインボリューション関数を鍵変換部における拡大鍵の生成に用いるとともに、暗号化鍵を鍵変換部で処理した結果を復号鍵とし、復号時には復号鍵を基にしてインボリューション関数を逆順に使用することで、拡大鍵の逆順生成を可能とするところにある。

【００１７】

本発明によれば、元の鍵をインボリューション関数で変換していくということ以外に鍵変換部で使用すべき関数に制約がなく、さらに暗号化鍵を復号鍵が同一である必要もないため、鍵変換部に使用できる関数の制約が極めて少ない。した

がって、安全性の高い拡大鍵を生成できるような関数を選択して鍵変換部を構成することが可能である。さらに復号鍵から拡大鍵を逆順生成できるため、暗号化処理と復号化処理で同一の鍵変換部を用いることができ、装置の回路規模をより小さくすることができる。

【００１８】

また発明者らが本発明に至ったのは、秘密鍵暗号方式において、非対称な鍵を用いるという発想の逆転を図ったところにある。

そもそも暗号化アルゴリズムは、暗号化と復号に同じ鍵を用いるか否かに応じて対称鍵暗号と非対称鍵暗号に分類できる。また暗号鍵を公開することで暗号を解読できるかどうかで秘密鍵暗号と公開鍵暗号に分類できる。

【００１９】

この２つの分類組み合わせのうち、従来は対称鍵秘密鍵暗号と非対称鍵公開鍵暗号の２通りのみが知られていた。対称な公開鍵暗号は原理的に不可能であるが、非対称な秘密鍵暗号は原理的には可能である。しかしながら、非対称な秘密鍵暗号にしたのでは、一つの暗復号処理のために複数の秘密鍵を管理する必要があるため、対管理コスト等の面から不利である。また、いかにして非対称な秘密鍵暗号を実現させるかいう問題もある。したがって、従来技術ではこのような方式は採用されていなかった。

【００２０】

これに対し本発明では、非対称であっても一つの秘密鍵（暗号化鍵若しくは復号鍵）を所持していれば暗号化復号ともに可能とし、これにより複数秘密鍵管理の問題を回避して現実的な非対称秘密鍵暗号を実現したのである。これは、暗号化鍵で暗号化された暗号文は復号鍵により復号でき、復号鍵で暗号化された暗号文は暗号化鍵により復号できることによっている。

【００２１】

すなわち一方が暗号化鍵のみを所持し、他方が当該暗号化鍵を鍵変換部で変換して出力された復号鍵のみを所持している場合には、次のようになる。まず、一方が自己の暗号化鍵で平文から暗号化した暗号文は、他方の復号鍵で逆順処理することで平文に戻すことができる。次に、他方の復号鍵で暗号化した暗号文は、

一方の暗号化鍵で逆順処理すれば平文に復号できるのである。

【００２２】

次に、本発明の具体的な実現手段について説明する。

まず、請求項１に対応する発明は、暗号化用の鍵を用いて平文を暗号文に暗号化し、及び又は、復号用の鍵を用いて暗号文を平文に復号するデータ処理装置であって、鍵の何れか若しくはその鍵変換結果に基づいて、鍵変換処理及び拡大鍵の出力を行うインボリューションな複数の鍵変換関数を順次接続してなるとともに、鍵変換処理の結果を鍵変換関数間で順次又は逆順に引き渡す鍵変換部と、拡大鍵を用いて暗号化処理及び又は復号処理を行うインボリューションな複数のラウンド関数を順次接続してなるとともに、ラウンド関数での処理結果をラウンド関数間で順次又は逆順に引き渡す攪拌部とを備えたデータ処理装置である。

【００２３】

このデータ処理装置は、暗号化装置にも復号装置にも使用できるメインの処理回路となる。すなわち鍵及びデータを順次処理すれば、データ暗号化が実現でき、鍵及びデータを逆順処理すれば、データ復号が実現できる。このような処理が可能なのは、上述したように、鍵変換関数及びラウンド関数がインボリューションであることによっている。

【００２４】

したがって、本発明を暗復号装置に利用すれば、装置規模の小さいコンパクトな暗復号装置を実現することができる。

次に、請求項２に対応する発明は、請求項１に対応する発明において、鍵変換関数は、第１の鍵又はその鍵変換結果を鍵変換処理の対象とするとともに、第２の鍵を用いて前記鍵変換処理を行うデータ処理装置である。

【００２５】

本発明によれば、鍵変換部の処理が攪拌部と同様な処理構成となり、弱鍵等となる可能性が極めて低い拡大鍵を出力することができる。したがって、暗号強度を高いものとすることができる。

【００２６】

次に、請求項３に対応する発明は、請求項２に対応する発明において、第２の

鍵は、暗号化用の鍵、及び又は、復号用の鍵に含まれるデータ処理装置である。

次に、請求項４に対応する発明は、請求項３に対応する発明において、第２の鍵には複数の種類が設けられ、暗号化用の鍵、及び又は、復号用の鍵は、当該複数種類の第２の鍵を含むことを可能として可変長の鍵としたデータ処理装置である。

【００２７】

次に、請求項５に対応する発明は、請求項１～４に対応する発明において、鍵変換関数は、攪拌部と同一のラウンド関数を含むデータ処理装置である。したがって、鍵変換関数に例えば非線形処理を行う関数を用いれば、暗号強度を高いものとすることができる。

【００２８】

次に、請求項６に対応する発明は、請求項１乃至５のうち、何れか一項記載のデータ処理装置を備えるとともに、暗号化用の鍵でありかつ復号用の鍵である一の鍵を保持する一の通信装置と、請求項１乃至５のうち、何れか一項記載のデータ処理装置を備えるとともに、一の鍵を鍵変換部で鍵変換処理した結果である他の鍵を暗号化用の鍵でありかつ復号用の鍵として保持する他の通信装置とを備えた通信システムである。

【００２９】

本発明によれば、各通信装置は、１個の鍵を保持すれば、暗号化処理、復号処理の何れも行うことができる。なお、ここで、各通信装置が保持する秘密鍵は必ずしも同一のものとはならない。すなわちこの通信は非対称な秘密鍵暗号となる。

【００３０】

次に、請求項７～９に対応する発明は、それぞれ請求項１，２又は５に対応する発明をコンピュータに実現させるプログラムを記録した記録媒体である。

この請求項７～９の何れかの発明に対応する記録媒体から読み出されたプログラムにより制御されるコンピュータは、それぞれ請求項請求項１，２又は５のデータ処理装置として機能する。

【００３１】

【発明の実施の形態】

以下、本発明の実施の形態について説明する。

（発明の第１の実施の形態）

図１は本発明の第１の実施の形態に係るデータ処理装置における主要構成部の一例並びに暗号化アルゴリズムを示す図である。

【００３２】

このデータ処理装置は、パーソナルコンピュータやワークステーション等の計算機の暗復号処理部として構成されており、以下、各実施形態においてデータ処理装置というときは、暗号化処理と復号処理を行う暗復号装置を意味している。

【００３３】

この暗復号装置は、攪拌部１と鍵変換部２を主要構成とする。これらの部分１，２は暗号化と復号の双方に共通して用いられる。また、特に図示しないが、攪拌部１と鍵変換部２の前後に転置処理等を設けるようにしてもよい。

【００３４】

攪拌部１は、それぞれラウンドＲ１からラウンドＲｎまでｎラウンドの処理により平文３の暗号化を行って暗号文４を出力し、ラウンドＲｎからラウンドＲ１までの処理により暗号文４の復号を行って平文３を出力する。攪拌部１には、各ラウンドＲ１～Ｒｎに対応して、ラウンド関数ｆｒ１～ｆｒｎ（単にラウンド関数ｆｒとも呼ぶ）が設けられている。

【００３５】

ラウンド関数ｆｒは、平文３若しくは中間的な暗号化結果７と鍵変換部２からの拡大鍵Ｋとを入力し、中間的な暗号化結果７若しくは暗号文４を出力する関数である。このラウンド関数ｆｒ１～ｆｒｎは、例えばＤＥＳ方式におけるラウンド関数と同様なものが用いられ、順にカスケード接続されている。

【００３６】

一方、鍵変換部２には、各ラウンドＲ１～Ｒｎに対応して、鍵変換関数ｆｋ１～ｆｋｎ（単に鍵変換関数ｆｋともいう）が設けられている。鍵変換関数ｆｋは

、暗号化鍵５若しくは中間的な鍵変換結果８を入力し、中間的な鍵変換結果８若しくは復号鍵６及び拡大鍵Ｋを出力する。すなわち鍵変換関数ｆｋ１～ｆｋｎは、攪拌部１のラウンド関数ｆｒ１～ｆｒｎに対し、それぞれ拡大鍵Ｋ１～Ｋｎを与える。

【００３７】

鍵変換関数ｆｋ１～ｆｋｎは、順にカスケード接続されている。したがって、鍵変換部２の第１ラウンドＲ１側から入力された暗号鍵５は最終ラウンドＲｎ側から復号鍵６として出力される。この復号鍵６及び上記暗号文４を最終ラウンドＲｎ側から入力すれば、第１ラウンドＲ１側から暗号化鍵５及び平文３が出力される。この様子を図２に示す。

【００３８】

図２は本実施形態に係るデータ処理装置における主要構成部の一例並びに復号アルゴリズムを示す図である。

なお、本明細書では、最初の平文３の暗号化に使用する鍵を暗号化鍵５と呼び、その最初の暗号化の結果に出力された鍵を復号鍵６と呼んでいる。しかし、本発明では、暗号化鍵５及び復号鍵６という呼称に関係なく、第１ラウンドＲ１側から鍵が入力された場合にその鍵は平文暗号化用の鍵として機能し、最終ラウンドＲｎ側から鍵が入力された場合にその鍵は暗号文復号用の鍵として機能する。

【００３９】

したがって、例えば復号鍵６を第１ラウンドＲ１側から入力すれば当該復号鍵６は平文暗号化用の鍵として機能し、暗号化鍵５を最終ラウンドＲｎ側から入力すれば当該暗号化鍵５は暗号文復号用の鍵として機能する。なお、暗号化鍵５及び復号鍵６はあくまでペアであり、上記場合では、それぞれ最終ラウンドＲｎ側及び第１ラウンドＲ１側から暗号化鍵５及び復号鍵６が出力される。したがって、対となる暗号化鍵若しくは復号鍵によってのみ、その暗号文の復号が可能である。以下の説明では、便宜上、第１ラウンドＲ１側から入力する鍵のことを単に暗号化鍵５、最終ラウンドＲｎ側から入力する鍵のことを単に復号鍵６と呼ぶ場合もある。

【００４０】

暗号化鍵５及び復号鍵６がこのような関係となるのは、鍵変換部２に設けられる鍵変換関数ｆｋの性質によるものである。この内容について説明する。

すなわち各鍵変換関数ｆｋは、インボリューション関数で構成されている。インボリューション関数とは、双方向関数の一種であり、変換と逆変換が同一である関数のことである。各鍵変換関数ｆｋにおいて変換と逆変換が同一であるがゆえに、上記暗号化鍵５と復号鍵６との関係が実現されるのである。なお、双方向関数は、全射でかつ単射となる写像間の変換に用いられる関数である。

【００４１】

インボリューション関数は、暗号化変換と復号変換で回路を共通化することが可能となるので暗号化アルゴリズムでよく用いられている。本発明においてはラウンド関数ｆｒのみならず、鍵変換関数ｆｋもインボリューションとしていることが特徴である。

【００４２】

また、インボリューション関数には種々のものがあるが、鍵変換関数ｆｋに用いられるものとしては、ＤＥＳのラウンド関数内の非線形関数ｆ（Ｒ，Ｋ）のように、ビット攪拌能力が高いものが望ましい。

【００４３】

次に、以上のように構成された本実施形態におけるデータ処理装置の動作について説明する。

まず、暗号化時には、図１に示すように、入力された暗号化鍵５は１ラウンドづつ鍵変換関数ｆｋにより拡大鍵Ｋと中間的な鍵変換結果９に変換され、最終的に復号鍵６に変換される。

【００４４】

このとき、平文３は、鍵変換部２の出力である拡大鍵Ｋを用いるラウンド関数ｆｒにより攪拌部１において１ラウンドづつ変換され、中間的な暗号化結果７を経て最終的に暗号文４に変換される。

【００４５】

一方、復号時には、図２に示すように、暗号文４を入力した攪拌部１において

暗号化時とは逆順に復号処理が行われ、中間的な復号結果９が出力されつつ、最終的には平文３が出力される。また、鍵変換部２においても同様に、復号鍵６が入力され、暗号化時とは逆順に鍵変換処理が行われ暗号鍵５が出力される。すなわち図１で見れば、暗号化時と比べて入出力が上下で逆転する。図２は、処理の関係を上下逆にして示しただけであり、攪拌部１及び鍵変換部２は図１に示すものと同一の回路が使用されている。

【００４６】

上述したように、本発明の実施の形態に係るデータ処理装置は、全単射な写像である鍵変換関数ｆｋをカスケードに接続した鍵変換部２を設けて、入力した鍵から各拡大鍵Ｋを出力し、またラウンド関数ｆｒをカスケードに接続した攪拌部１を設け、これに平文若しくは暗号文及び拡大鍵Ｋを入力して暗号文若しくは平文を出力するようにしたので、必ずしも同一でない暗号鍵と復号鍵を使用した暗号化及び復号を実現し、これにより暗復号のための回路として同一の攪拌部１及び鍵変換部２を用いることができる。

【００４７】

したがって、暗号化装置と復号装置の主要部分を完全に共通化させることができ、装置規模を小さくすることができる。

なお、従来の秘密鍵暗号化アルゴリズムでは暗号化鍵と復号鍵が同一であり、本発明のように鍵変換部の出力結果が暗号化鍵と異なる復号鍵であるといったことはないが、暗号化鍵と復号鍵が必ずしも一致しないことということはない。

【００４８】

また、鍵変換関数ｆｋとしては、インボリューション関数でさえあれば、種々の関数を選択することができるので、例えば非線形なデータ攪拌能力が高い関数を使用すれば、暗号化強度を高めることができ、より一層安全性の高いものとすることができる。

（発明の第２の実施の形態）

本実施形態は、第１の実施形態における鍵変換部及び使用する鍵の具体的な構成例を示すものである。

【００４９】

図３は本発明の第２の実施の形態に係るデータ処理装置における鍵変換部の構成例を示すブロック図であり、図１又は図２と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【００５０】

このデータ処理装置は、鍵変換部２において鍵変換関数ｆｋにパラメータＰ１，Ｐ２及びＰ３の何れかが入力され、このパラメータを用いて拡大鍵Ｋを生成するようになっている他、第１の実施形態と同様に構成されている。

【００５１】

本実施形態では、鍵５，６が可変長であり、データ部１１，１３とパラメータ部１２，１４から構成されている。

暗号化鍵５のデータ部１１は変換される対象データＤからなり、パラメータ部１２は変換パラメータＰ１，Ｐ２及びＰ３からなっている。すなわち本実施形態の鍵５，６は、データ部とパラメータ部のそれぞれを鍵と考えれば、２つの鍵からなっているといえる。また、パラメータ部には複数のパラメータが格納できるので、さらに多数の鍵からなるものであるともいえる。

【００５２】

一方、復号鍵６のデータ部１３は変換後のデータＤ′からなり、パラメータ部１２は変換パラメータＰ１′，Ｐ２′及びＰ３′からなっている。

なお、図３では理解のしやすさのために、データＤとパラメータＰ１，Ｐ２及びＰ３とを順に分けて示しているが、ビット順番を入れ替えたものを使用してもよい。この鍵はパラメータ部１１が複数の変換パラメータを持つことで、可変長の鍵を実現する。パラメータ数は同図に示すように三つに限らず、さらに多数でもよい。

【００５３】

鍵変換関数ｆｋは、暗号化鍵５のデータＤ若しくは中間的な鍵変換の結果８および何れかのパラメータＰ１，Ｐ２又はＰ３を入力し、中間的な鍵変換の結果８若しくは復号鍵６のデータＤ′及び拡大鍵Ｋを出力する。つまり、本実施形態の鍵変換部２及び鍵変換関数ｆｋは、データＤ（若しくは中間的な鍵変換結果８）とパラメータＰの二つの鍵を入力できるようなっているともいえる。

【００５４】

次に、以上のように構成された本実施形態におけるデータ処理装置の動作について説明する。

まず、拡大鍵Ｋによる全体的な暗号化、復号の手順は第１の実施形態と同様である。

【００５５】

鍵変換部２における処理は次のようになる。

まず、入力された暗号化鍵５のデータＤは、変換パラメータＰ１，Ｐ２又はＰ３の何れかが入力された鍵変換関数ｆｋの処理により、各ラウンドＲにおける拡大鍵Ｋを出力しながら、１ラウンドづつ変換される。各ラウンドの変換を経て最終的には、復号鍵６のデータＤ′に変換され出力される。

【００５６】

複数の変換パラメータはラウンド毎に順次適用する。ラウンド数の方が大きい場合は、繰り返して適用する。この繰り返し適用は本実施形態ではサイクリックなものとしたが、その他の適用規則を設けてもよい。

【００５７】

なお、復号鍵６のパラメータ部１４には、暗号化鍵５のパラメータをそのまま格納してもよく、また、これに所定の処理を施したものを格納してもよい。

上述したように、本発明の実施の形態に係るデータ処理装置は、第１の実施形態と同様な構成を設けた他、暗号化鍵５及び復号鍵６に鍵本体であるデータＤ，Ｄ′といわば第２の鍵であるパラメータＰ，Ｐ′を含ませ、鍵変換関数にデータＤ（若しくは中間的な鍵変換結果８）とパラメータＰの２種類の鍵を入力するようにしたので、第１の実施形態と同様な効果が得られる他、解読困難な拡大鍵Ｋを生成することができ、暗号の安全性を一層高めることができる。

【００５８】

また、本実施形態のデータ処理装置では、例えばパラメータ数を変更することで、鍵の長さを可変としたので、これによっても暗号の安全性を高めることができる。

（発明の第３の実施の形態）

本実施形態は、第２の実施形態における鍵変換部の具体的な構成例を示すものである。

【００５９】

図４は本発明の第３の実施の形態に係るデータ処理装置における鍵変換関数の構成例を示すブロック図であり、図１～図３と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【００６０】

このデータ処理装置は、鍵変換関数ｆｋが以下に説明するように構成される他、第２の実施形態と同様に構成されている。

暗号化鍵５は、第２の実施形態と同様に、変換される対象のデータＤと変換パラメータＰを含んでいる。

【００６１】

鍵変換関数ｆｋは、入力されたデータＤ若しくは中間的な鍵変換結果８を変換して拡大鍵Ｋを出力する変換関数２１と、インボリューション関数でありかつデータ攪拌能力が高いラウンド関数２２とを備えている。

【００６２】

ラウンド関数２２は、攪拌部１と同じラウンド関数が用いられる。このラウンド関数２２には、データＤ若しくは中間的な鍵変換結果８と変換パラメータＰとが入力され、データＤ等にデータ変換を施して、中間的な鍵変換結果８若しくは最終的な変換データＤ′を出力する。ここで、攪拌部１のラウンド関数ｆｒにおける拡大鍵Ｋの入力がパラメータＰの入力に相当する。

【００６３】

ラウンド関数２２の出力結果８は、次ラウンドの鍵変換関数ｆｋに対する入力であり、また、拡大鍵Ｋは前ラウンドにおけるラウンド関数２２のデータ入力に変換関数２１による処理を施したものとなる。

【００６４】

変換関数２１では例えばビットの並び替え等の処理を行う。なお、この変換関数２１は省略することもできる。

ここで、拡大鍵Ｋはラウンド関数２２の出力側の信号を元に作成しない方が有

利である点に留意する。少なくとも本実施形態では必ずラウンド関数２２の入力側の信号を元に拡大鍵Ｋを作成する。

【００６５】

これは、鍵へ変換関数２１の１段目の出力がデータＤとパラメータＰに依存しているが、ラウンド関数２２の出力側の信号を利用した場合、同じ出力を与えるデータＤとパラメータＰの他の値が存在することが数学的に証明できるからである。この事実は、暗号アルゴリズムの安全性に悪影響を与える。すなわち入力側信号を用いた場合、鍵のデータＤと、パラメータＰの一番最初のものの二つを正しい鍵以外から選べることになるので鍵の探索が容易になり、安全性が低くなる。

【００６６】

次に、このように構成された本実施形態におけるデータ処理装置の動作について説明する。

まず、鍵変換関数ｆｋへの入力データには変換関数２１による処理が施されて、拡大鍵として出力される。一方、同入力データがラウンド関数２２によりデータ攪拌されて次の鍵変換関数ｆｋへ出力される。

【００６７】

以上の鍵変換関数内における処理を除けば、本実施形態のデータ処理装置は第２の実施形態と同様に動作する。

上述したように、本発明の実施の形態に係るデータ処理装置は、第２の実施形態と同様な構成を設けた他、鍵変換関数ｆｋに攪拌部１と同じラウンド関数２２を用いるようにしたので、上記実施形態と同様な効果が得られる他、鍵についてのデータ攪拌を強くして暗号の安全性を高めることができる。

【００６８】

また、鍵変換関数ｆｋにおいて、ラウンド関数２２への入力側のデータに基づいて拡大鍵Ｋを作成するようにしたので、同一の拡大鍵Ｋが生じることがなく暗号強度の高い暗号化を実現することができる。

【００６９】

なお、本実施形態の変形例として、最終ラウンドの鍵変換関数ｆｋにおけるラ

ウンド関数２２を省略することが可能である。本実施形態では、ラウンド関数２２へ入力前のデータに基づき拡大鍵Ｋを作成するからである。この場合には、最終段の出力である復号鍵はラウンド関数を適用しないで出力するので、計算時間が節約できるという利点がある。

（発明の第４の実施の形態）

本実施形態は、第１の実施形態における鍵変換部の他の構成例を示すものである。

【００７０】

図５は本発明の第４の実施の形態に係るデータ処理装置における鍵変換関数の構成例を示すブロック図であり、図１～図３と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【００７１】

このデータ処理装置は、鍵変換関数ｆｋが以下に説明するように構成される他、第１の実施形態と同様に構成されている。

この鍵変換関数ｆｋは、暗号化鍵５若しくは中間的な鍵変換結果８である入力データを変換して拡大鍵Ｋを出力する変換関数３１と、同入力データを変換して中間的な鍵変換結果８若しくは復号鍵６を出力する鍵変換部分から構成される。この鍵変換部分は、選択回路３２と、複数の変換関数３３（＃１，＃２，．．，＃ｍ）と、ＯＲゲート３４とから構成されている。

【００７２】

選択回路３２は、選択信号に基づき、入力データを変換する変換関数３３を選択し、選択した変換関数に入力データを引き渡す。

変換関数３３は、インボリューション関数であり、入力データを攪拌する。この関数３３には、攪拌部１のラウンド関数で用いられるような攪拌能力の高いものを使用する。

【００７３】

ＯＲゲート３４は、変換関数３３から出力された変換後のデータを外部に出力する。

次に、以上のように構成された本実施形態におけるデータ処理装置の動作につ

いて説明する。

【００７４】

まず、鍵変換関数ｆｋに入力されたデータは変換関数３１により変換されて、拡大鍵Ｋとして出力される。一方、この入力データは選択回路３２に与えられた選択信号に基づき、複数の変換関数３３の何れかに入力される。

【００７５】

次に、選択された変換関数３３により、入力データが変換される。この変換関数３３により変換されたデータは、ＯＲゲート３４により１つの信号にまとめられ出力される。この出力データは次ラウンドの鍵変換関数ｆｋに入力されるか、復号鍵として出力される。

【００７６】

以上の鍵変換関数内における処理を除けば、本実施形態のデータ処理装置は第１の実施形態と同様に動作する。

上述したように、本発明の実施の形態に係るデータ処理装置は、第１の実施形態と同様な構成を設けた他、鍵変換関数ｆｋに複数の変換関数３３を設け、その何れかを選択して暗号化鍵を変換していくようにしたので、第１の実施形態と同様な効果が得られる他、鍵変換結果を予想しにくいものとすることができ、暗号の安全性を高めることができる。

（発明の第５の実施の形態）

本実施形態では、第１～第４の何れかの実施形態におけるデータ処理装置を用いた通信システムについて説明する。

【００７７】

図６は本発明の第５の実施の形態に係る通信システムにおける主要構成部の一例を示すブロック図であり、図１～図５と同一部分には同一符号を付してその説明を省略する。

【００７８】

この通信システムは、通信者Ａが用いる通信装置４１Ａと、通信者Ｂが用いる通信装置ＢとがインターネットやＬＡＮ等の通信路４０を介して接続されてなっている。

【００７９】

通信装置４１Ａは、データ通信手段を備えた計算機システムであり、暗復号装置４２と、暗号化鍵ファイル４３，平文ファイル４４及び暗号文ファイル４５を格納する記憶手段（図示せず）と、鍵送受信処理部４６と、通信処理部４７とから構成されている。

【００８０】

一方、通信装置４１Ｂは、暗号化鍵ファイル４３に代えて、復号鍵ファイル４８を有する他、通信装置４１Ｂと同様に構成されている。

すなわち通信装置Ａは、平文暗号化用及び暗号文復号用の鍵として暗号化鍵５のみを暗号化鍵ファイル４３に保持し、通信装置Ｂは、平文暗号化用及び暗号文復号用の鍵として復号鍵６のみを復号鍵ファイル４８に保持する。

【００８１】

暗復号装置４２は、第１～第４の何れかの実施形態における攪拌部１及び鍵変換部２を暗復号の共通部分として備えており、これに暗号化若しくは復号における前後処理や暗復号の選択、さらに処理制御用の回路等が付加されて構成される。図６では、暗号化処理の場合は左側から鍵や平文が暗復号回路４２に入力され、復号処理の場合は鍵や暗号文が右側から入力される。

【００８２】

なお、各通信装置４１Ａ，４１Ｂが保持する暗号化鍵５及び復号鍵６は対になったものであり、暗号化鍵５を鍵変換部２で変換して得られるのが復号鍵６であり、復号鍵６を鍵変換部２で逆順に変換して得られるのが暗号化鍵５である。

【００８３】

鍵送受信処理部４６は、通信装置４１Ａ，４１Ｂ間で鍵を授受するときに、安全に鍵の引き渡しを行うための手段である。

次に、以上のように構成された本実施形態における通信システムの動作について説明する。

【００８４】

あらかじめ通信者Ａと通信者Ｂは互いに暗号通信するための鍵を共有する必要がある。このために例えば、通信装置４１Ａで暗号文を作成する際にともに生成

された復号鍵６を、鍵送受信処理部４６により通信装置４１Ｂ側に引き渡す。この引き渡された復号鍵６は、復号鍵ファイル４８に格納される。

【００８５】

図７は本実施形態における通信の様子を説明する図である。

図６及び図７を用いて、まず、通信者Ａから通信者Ｂへの暗号通信の様子を説明する。

【００８６】

まず、通信者Ａは暗号化通信したい平文５１を自分が所有する暗号化鍵５を使い暗号化する。このとき、図６に示す通信装置４１Ａでは、平文５１及び暗号化鍵５が暗復号装置４２の左側から入力され、第１ラウンドＲ１より順次変換される。この暗号化された暗号文５２は通信処理部４７、通信路４０を介して通信者Ｂに伝送される。

【００８７】

暗号文５２を受け取った通信者Ｂは自分が所有する復号鍵６を使い、暗号文５１を復号し平文５３を取り出す。この復号においては、復号鍵６と暗号文５２が通信装置４１Ｂにおける暗復号装置４２の左側から入力され、暗号化の時とは逆順に最終ラウンドＲｎから変換が行われる。

【００８８】

次に、通信者Ｂから通信者Ａへの暗号通信の様子を説明する。

まず、通信者Ｂは、暗号化通信したい平文５４を自分が所有する復号鍵６を使い暗号化する。このとき通信装置４１Ｂでは、復号鍵６と平文５４が通信装置４１Ｂにおける暗復号装置４２の右側から入力され、第１ラウンドＲ１から順に変換が行われる。

【００８９】

この暗号化された暗号文５５は通信者Ａの通信装置４１Ａに伝送され、通信者Ａは自分が所有する暗号化鍵５を使い、暗号文５５を復号し平文５６を取り出す。この復号においては、暗号化鍵５と暗号文５５が通信装置４１Ａにおける暗復号装置４２の右側から入力され、暗号化の時とは逆順に最終ラウンドＲｎから変換が行われる。

【００９０】

このように、通信者Ａは、暗号化送信する場合でも受信する場合でも、暗号化鍵５しか使っていない。同様に、通信者Ｂも、復号鍵６しか使用しない。したがって、暗号化鍵５と復号鍵６は異なる鍵であるが、その両方を所有する必要はなく、通信者が管理する鍵の数は１つのみである。

【００９１】

上述したように、本発明の実施の形態に係る通信システムは、第１～第４の実施形態における何れかの暗復号装置４２を備えた通信装置４１Ａ，Ｂにより暗号化通信を行うようにしたので、第１～第４の実施形態と同様な効果が得られる他、各通信者Ａ，Ｂは異なる鍵を所有するにもかかわらず各通信者が管理すべき鍵の数が増えず、鍵管理の容易なシステムとすることができる。

【００９２】

なお、実施形態に記載した手法は、計算機（コンピュータ）に実行させることができるプログラム（ソフトウエア手段）として、例えば磁気ディスク（フロッピーディスク、ハードディスク等）、光ディスク（ＣＤ－ＲＯＭ、ＤＶＤ等）、半導体メモリ等の記憶媒体に格納し、また通信媒体により伝送して頒布することもできる。なお、媒体側に格納されるプログラムには、計算機に実行させるソフトウエア手段（実行プログラムのみならずテーブルやデータ構造も含む）を計算機内に構成させる設定プログラムをも含むものである。本装置を実現する計算機は、記憶媒体に記録されたプログラムを読み込み、また場合により設定プログラムによりソフトウエア手段を構築し、このソフトウエア手段によって動作が制御されることにより上述した処理を実行する。

【００９３】

【発明の効果】

以上詳記したように本発明によれば、鍵変換部の各ラウンドの鍵変換関数にインボリューション関数を使用し、かつ、暗号化と復号に異なる鍵を使用するようにしたので、秘密鍵暗号の装置規模を小さくすることを可能とし、かつ鍵の安全性を高めることができ、さらには鍵管理も容易なものとすることができるデータ処理装置及び通信システム並びに記録媒体を提供することができる。

【図面の簡単な説明】

【図１】

本発明の第１の実施の形態に係るデータ処理装置における主要構成部の一例並びに暗号化アルゴリズムを示す図。

【図２】

同実施形態に係るデータ処理装置における主要構成部の一例並びに復号アルゴリズムを示す図。

【図３】

本発明の第２の実施の形態に係るデータ処理装置における鍵変換部の構成例を示すブロック図。

【図４】

本発明の第３の実施の形態に係るデータ処理装置における鍵変換関数の構成例を示すブロック図。

【図５】

本発明の第４の実施の形態に係るデータ処理装置における鍵変換関数の構成例を示すブロック図。

【図６】

本発明の第５の実施の形態に係る通信システムにおける主要構成部の一例を示すブロック図。

【図７】

同実施形態における通信の様子を説明する図。

【図８】

ＤＥＳ方式を説明する図。

【符号の説明】

１…攪拌部

２…鍵変換部

３，５１，５３，５４，５６…平文

４，５２，５５…暗号文

５…暗号化鍵

６…復号鍵

７…中間的な暗号化結果

８…中間的な鍵変換結果

１１…暗号化鍵のデータ部

１２…暗号化鍵の変換パラメータ部

１３…復号鍵のデータ部

１４…復号鍵の変換パラメータ部

２１…変換関数

２２…ラウンド関数

３１…変換関数

３２…選択回路

３３…変換関数

３４…ＯＲゲート

４０…通信路

４１Ａ…通信装置

４１Ｂ…通信装置

４２…暗復号装置

４３…暗号化鍵ファイル

４４…平文ファイル

４５…暗号文ファイル

４６…鍵送受信処理部

４７…通信処理部

４８…復号鍵ファイル

Ａ，Ｂ…通信者

Ｄ，Ｄ′…データ

ｆｋ１～ｆｋｎ，ｆｋ…鍵変換関数

ｆｒ１～ｆｒｎ…ラウンド関数

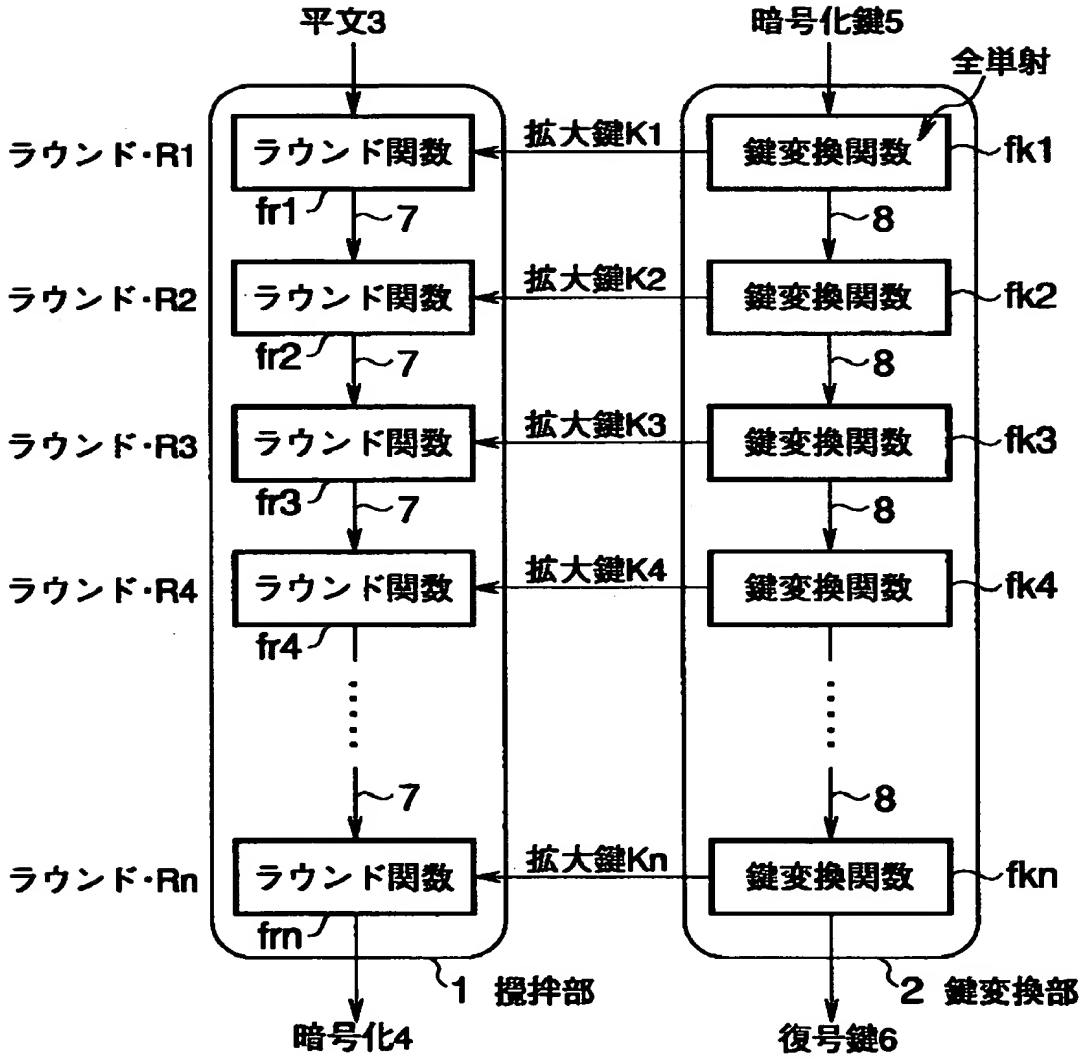
Ｋ１～Ｋｎ，Ｋ…拡大鍵

Ｐ１，Ｐ２，Ｐ３，Ｐ１′，Ｐ２′，Ｐ３′…変換パラメータ

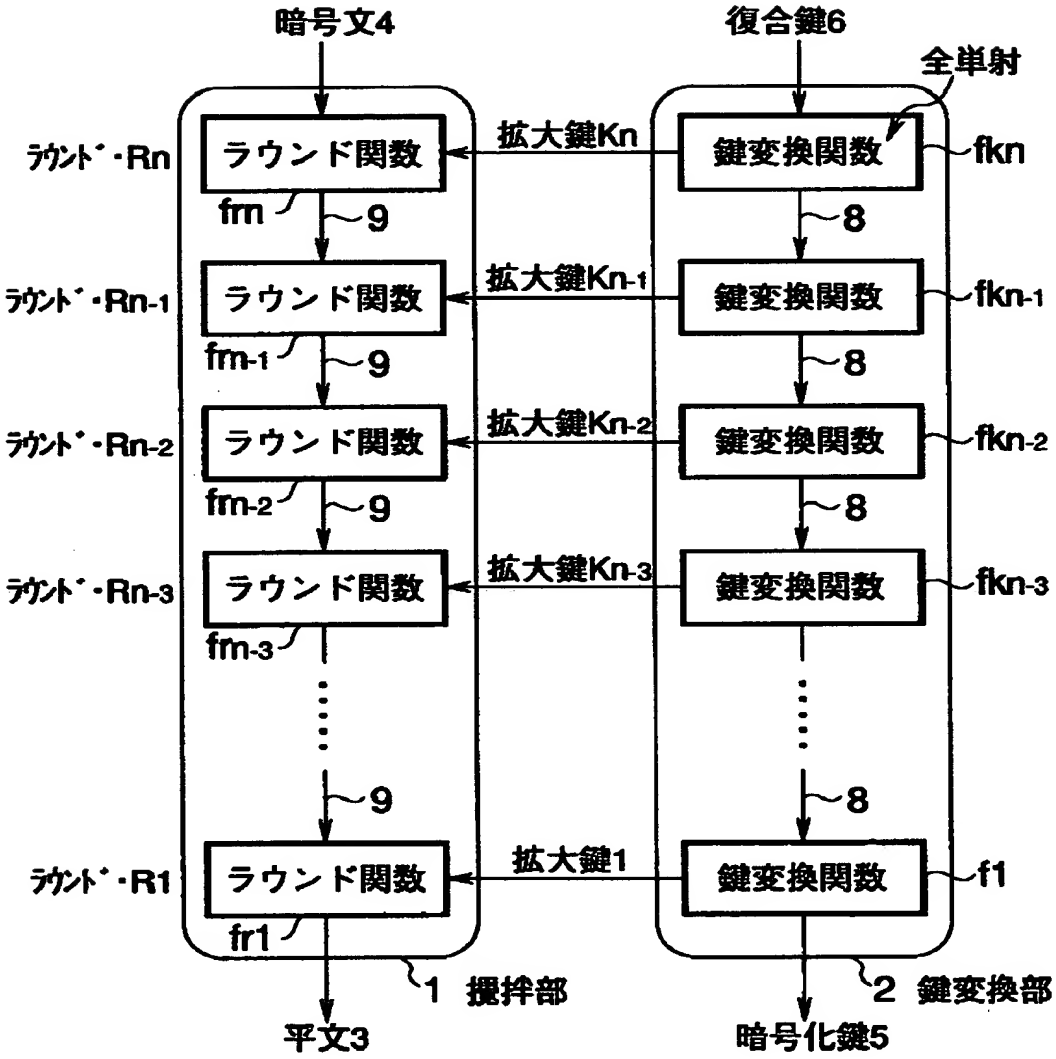
Ｒ１～Ｒｎ…ラウンド

【書類名】　　図面

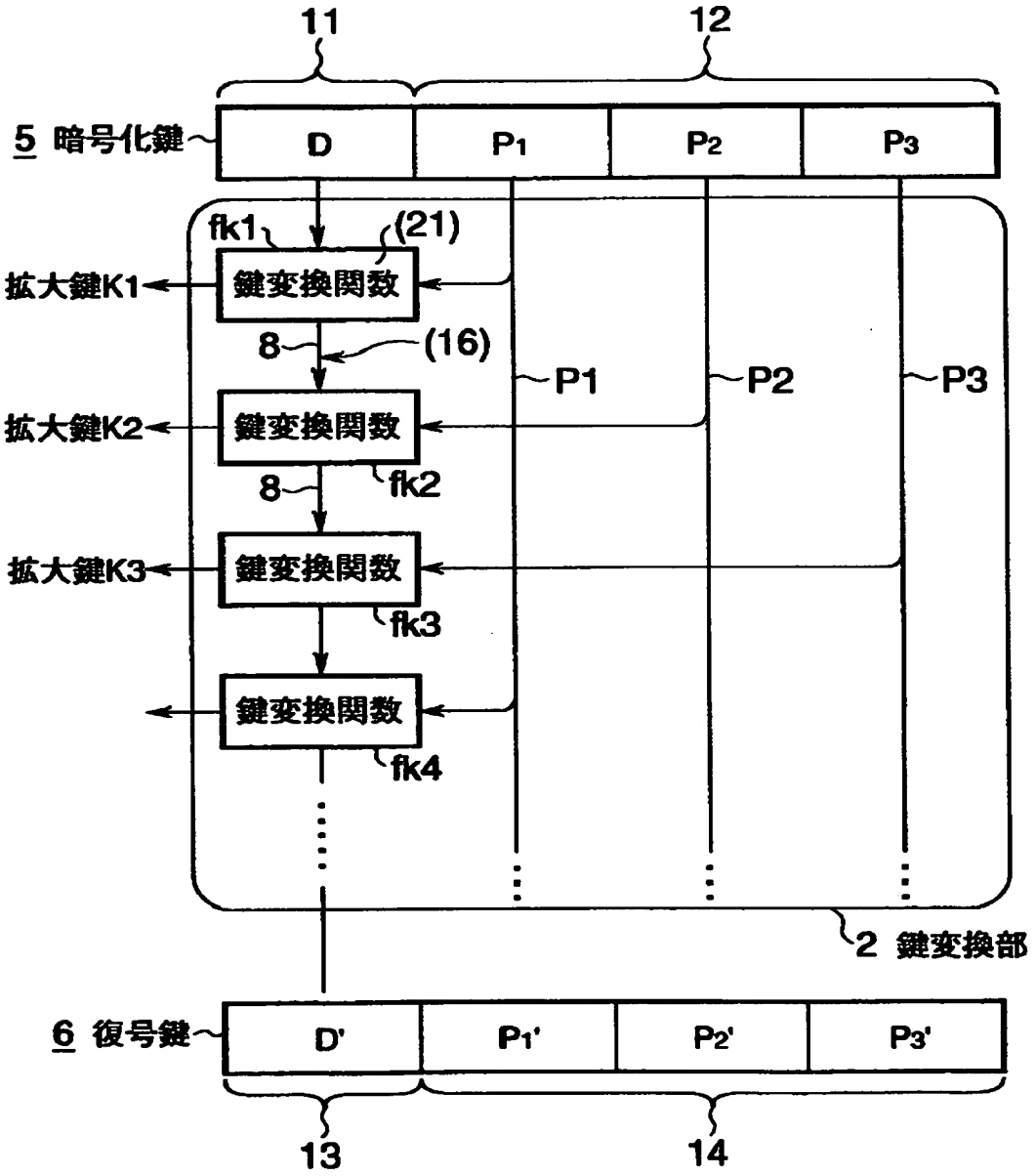
【図１】


平文3
暗号化鍵5
全単射
ラウンド・R1
ラウンド関数
拡大鍵K1
鍵変換関数
fk1
fr1
7
8
ラウンド・R2
ラウンド関数
拡大鍵K2
鍵変換関数
fk2
fr2
7
8
ラウンド・R3
ラウンド関数
拡大鍵K3
鍵変換関数
fk3
fr3
7
8
ラウンド・R4
ラウンド関数
拡大鍵K4
鍵変換関数
fk4
fr4
7
8
ラウンド・Rn
ラウンド関数
拡大鍵Kn
鍵変換関数
fkn
frn
1 攪拌部
2 鍵変換部
暗号化4
復号鍵6

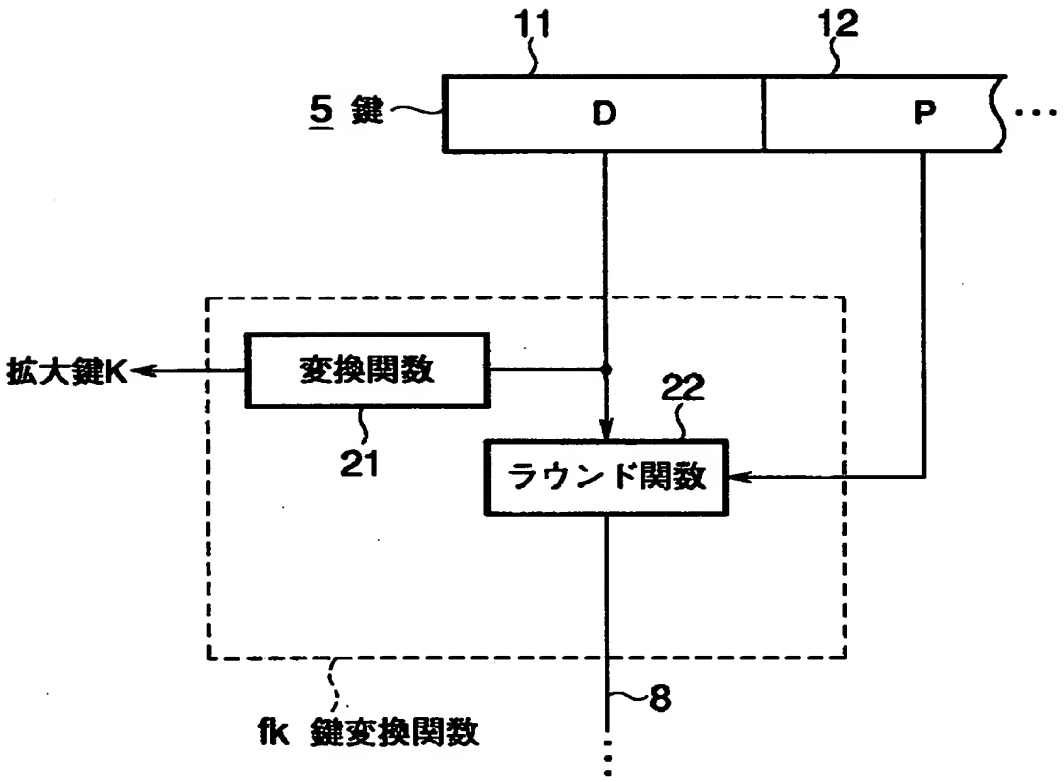
【図２】


暗号文4
復合鍵6
全単射
ﾗｳﾝﾄﾞ・Rn
ラウンド関数
拡大鍵Kn
鍵変換関数
fkn
fm
9
8
ﾗｳﾝﾄﾞ・Rn-1
ラウンド関数
拡大鍵Kn-1
鍵変換関数
fkn-1
fm-1
9
8
ﾗｳﾝﾄﾞ・Rn-2
ラウンド関数
拡大鍵Kn-2
鍵変換関数
fkn-2
fm-2
9
8
ﾗｳﾝﾄﾞ・Rn-3
ラウンド関数
拡大鍵Kn-3
鍵変換関数
fkn-3
fm-3
9
8
ﾗｳﾝﾄﾞ・R1
ラウンド関数
拡大鍵1
鍵変換関数
f1
fr1
1 攪拌部
2 鍵変換部
平文3
暗号化鍵5

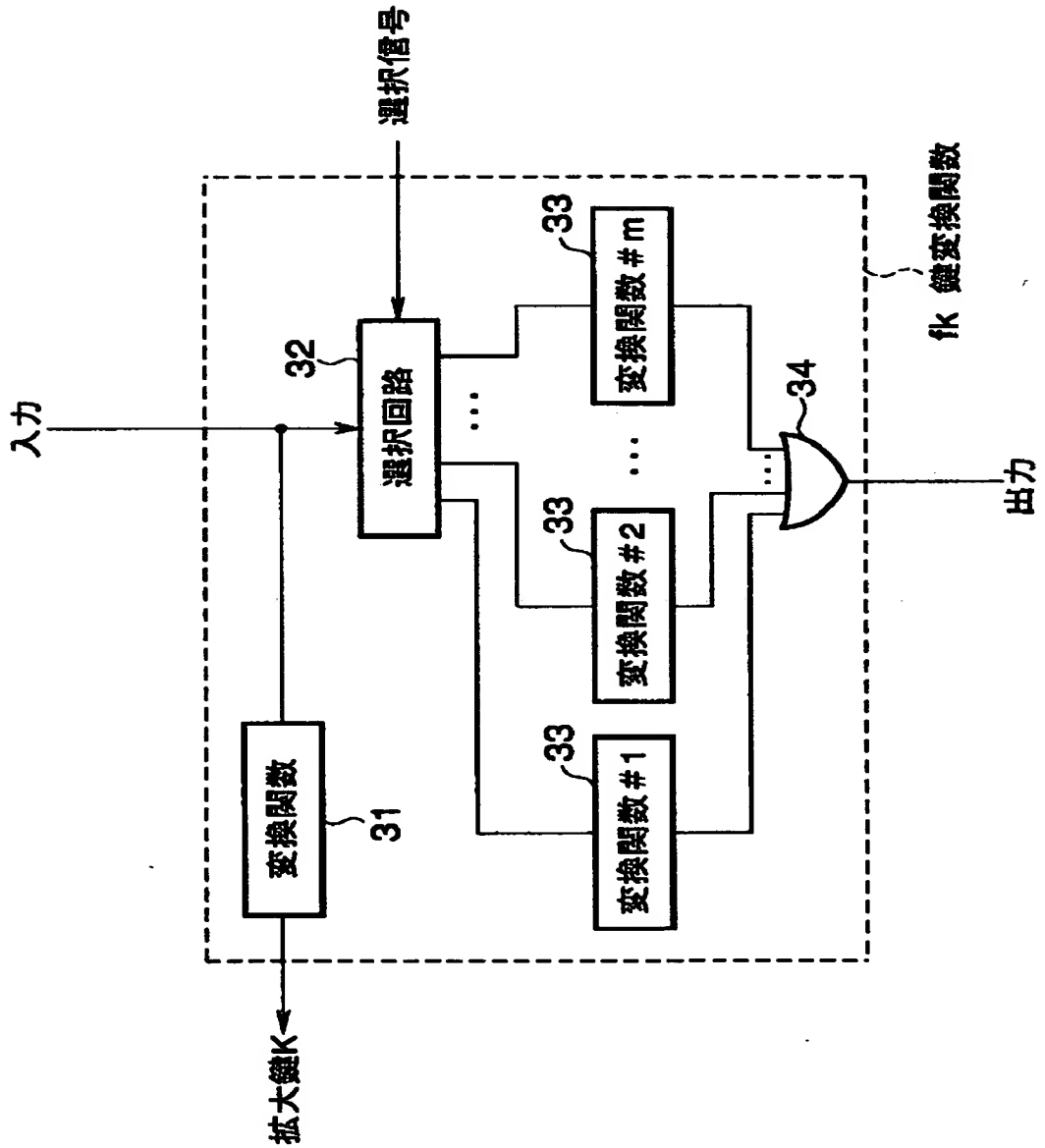
【図３】


11
12
5 暗号化鍵
D
P1
P2
P3
fk1
(21)
拡大鍵K1
鍵変換関数
8
(16)
P1
P2
P3
拡大鍵K2
鍵変換関数
8
fk2
拡大鍵K3
鍵変換関数
fk3
鍵変換関数
fk4
2 鍵変換部
6 復号鍵
D'
P1'
P2'
P3'
13
14

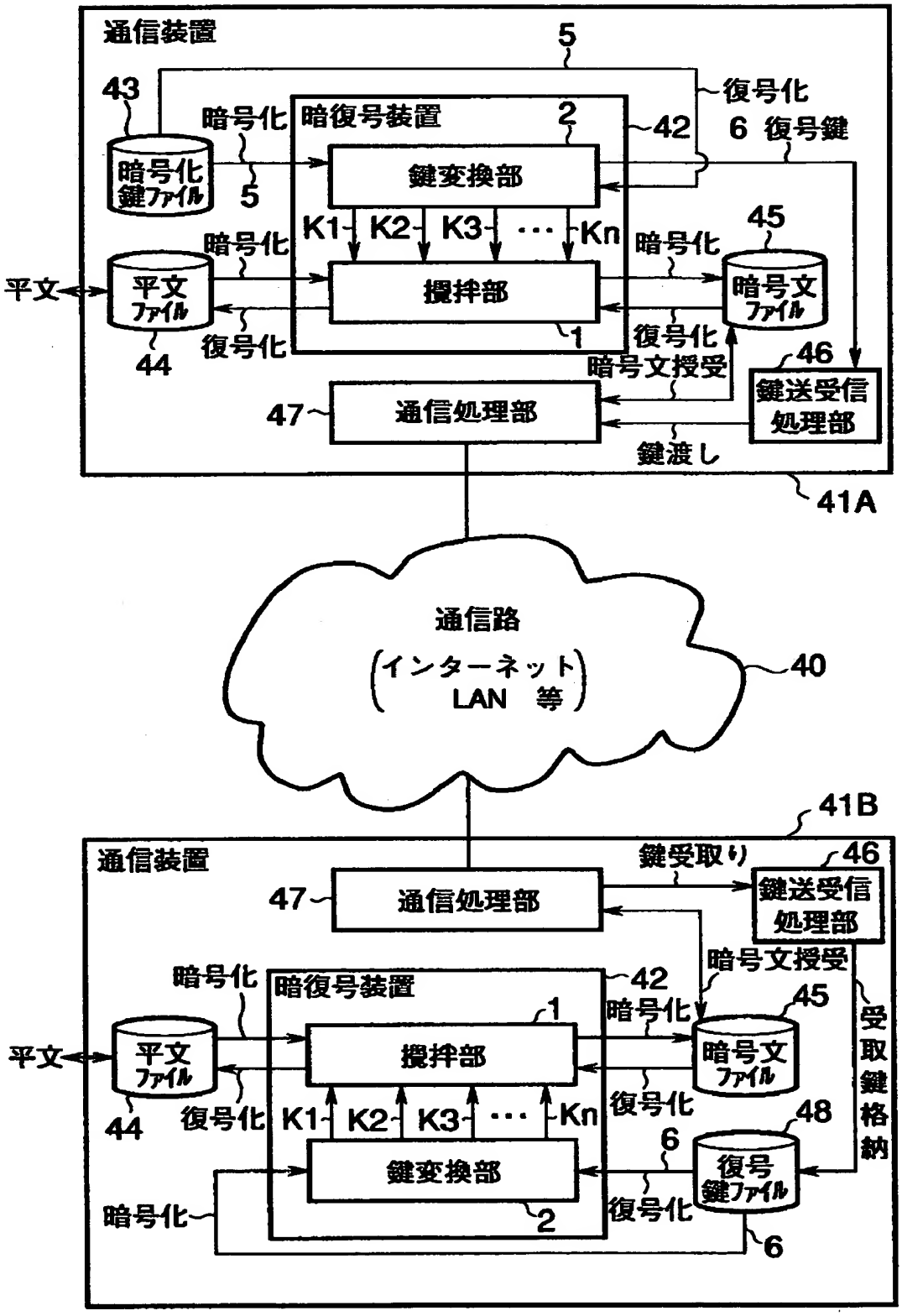
【図４】



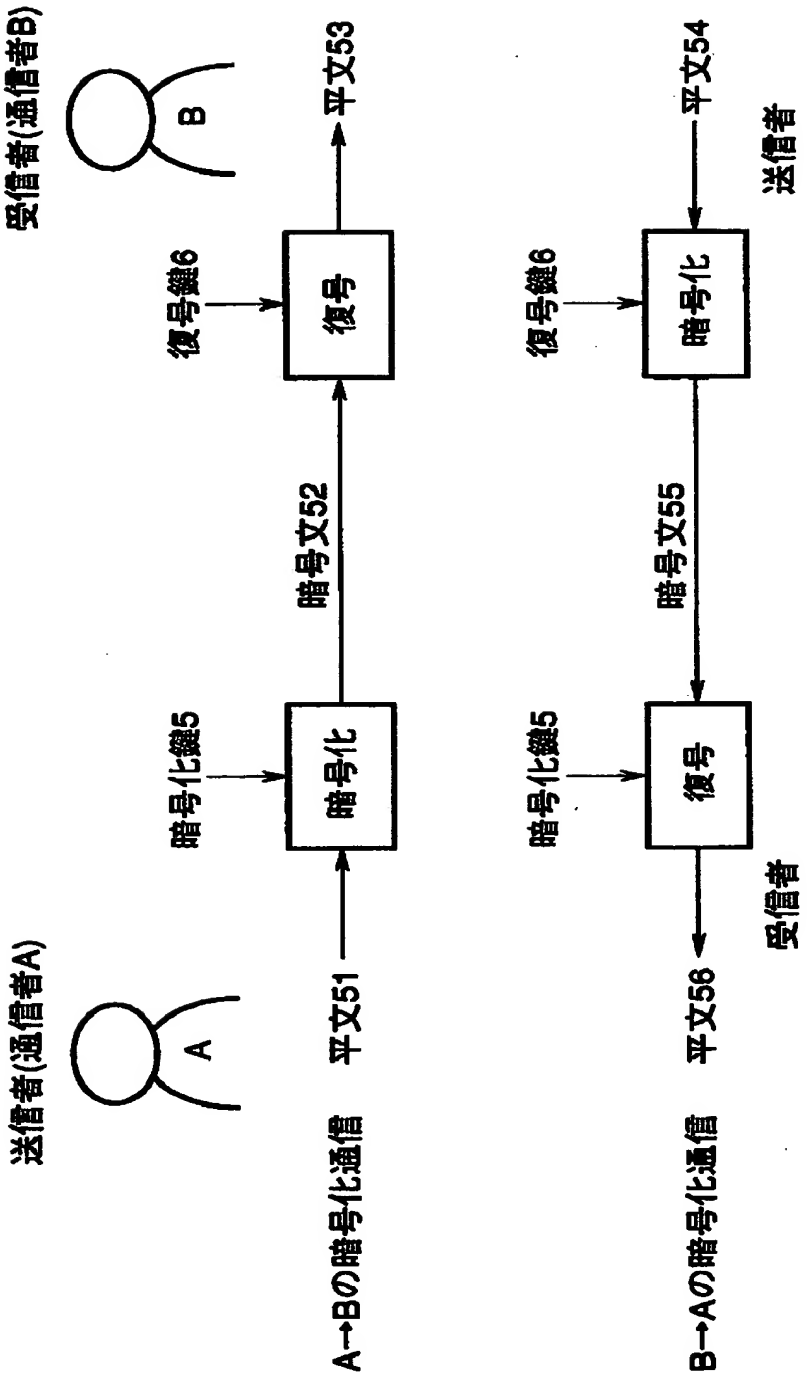
【図５】


選択信号
入力
32
選択回路
33
変換関数＃m
33
変換関数＃2
33
変換関数＃1
34
出力
K 鍵変換関数
変換関数
31
拡大鍵K

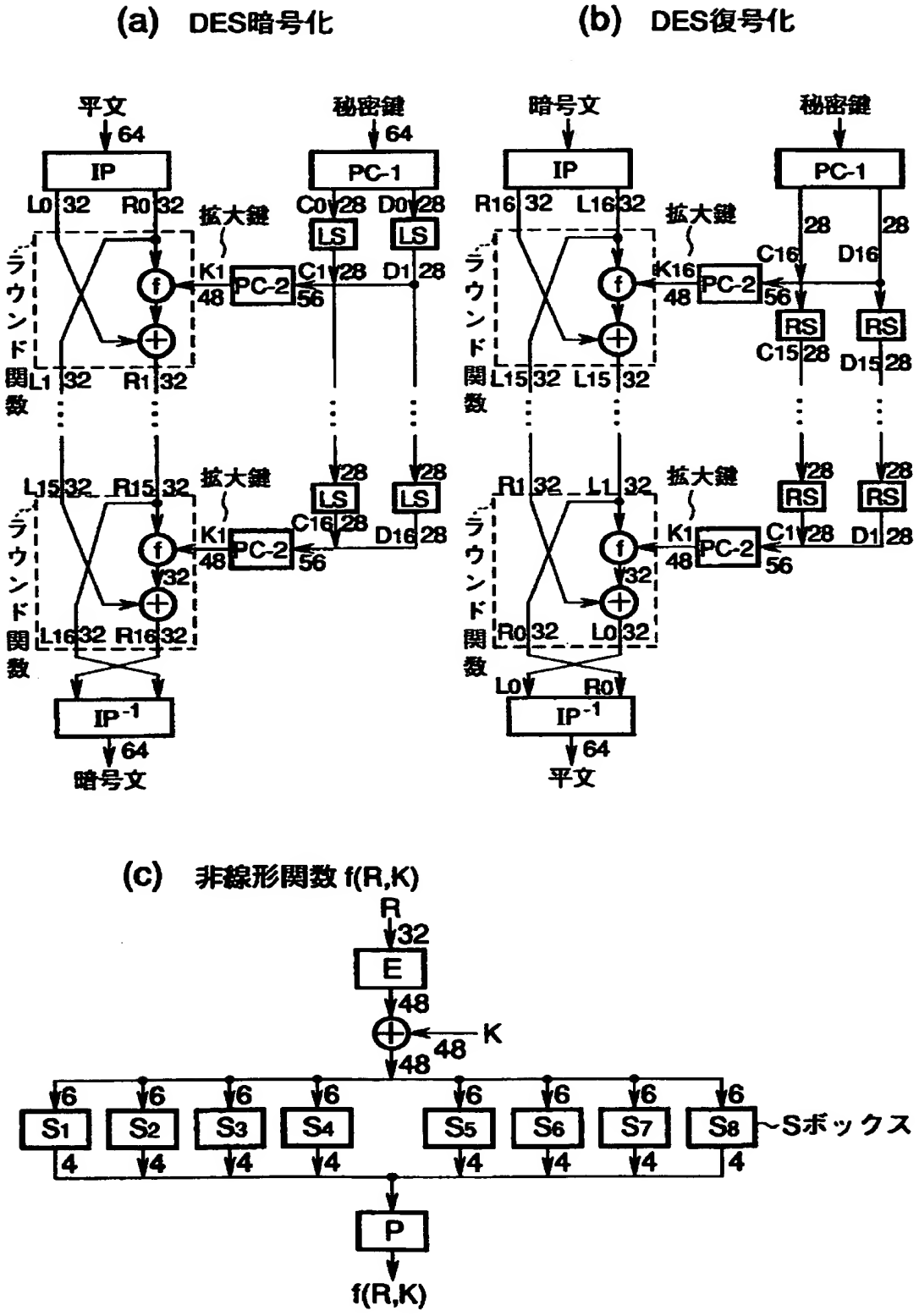
【図６】


通信装置
5
43
暗号化
暗復号装置
2
42
復号化
6 復号鍵
暗号化鍵ファイル
5
鍵変換部
K1
K2
K3
・・・
Kn
45
暗号化
暗号化
平文
平文ファイル
攪拌部
暗号文ファイル
1
復号化
44
復号化
暗号文授受
46
鍵送受信処理部
47
通信処理部
鍵渡し
41A
通信路
(インターネット
LAN 等)
40
41B
通信装置
鍵受取り
46
47
通信処理部
鍵送受信処理部
暗号文授受
暗号化
暗復号装置
42
1
暗号化
45
受取鍵格納
平文
平文ファイル
攪拌部
暗号文ファイル
復号化
44
復号化
K1
K2
K3
・・・
Kn
48
6
鍵変換部
復号鍵ファイル
暗号化
2
復号化
6

【図７】


送信者(通信者A)
A
受信者(通信者B)
B
暗号化鍵5
暗号化
復号鍵6
復号
平文51
暗号文52
平文53
A→Bの暗号化通信
暗号化鍵5
復号
復号鍵6
暗号化
平文54
暗号文55
平文56
B→Aの暗号化通信
送信者
受信者

【図８】


(a) DES暗号化
(b) DES復号化
(c) 非線形関数 f(R,K)
平文
暗号文
秘密鍵
IP
IP-1
PC-1
PC-2
拡大鍵
ラウンド関数
LS
RS
f
E
P
S1
S2
S3
S4
S5
S6
S7
S8
Sボックス
f(R,K)

【書類名】　　要約書

【要約】

【課題】　秘密鍵暗号の装置規模を小さくすることを可能とし、かつ鍵の安全性を高めることができ、さらには鍵管理も容易なものとすることができる。

【解決手段】　暗号化用の鍵を用いて平文を暗号文に暗号化し、及び又は、復号用の鍵を用いて暗号文を平文に復号するデータ処理装置であって、鍵の何れか若しくはその鍵変換結果に基づいて、鍵変換処理及び拡大鍵の出力を行うインボリューションな複数の鍵変換関数ｆｋを順次接続してなるとともに、鍵変換処理の結果を鍵変換関数間で順次又は逆順に引き渡す鍵変換部２と、拡大鍵を用いて暗号化処理及び又は復号処理を行うインボリューションな複数のラウンド関数を順次接続してなるとともに、ラウンド関数ｆｒでの処理結果をラウンド関数間で順次又は逆順に引き渡す攪拌部１とを備えたデータ処理装置。

【選択図】　　図１

【書類名】　職権訂正データ
【訂正書類】　特許願

＜認定情報・付加情報＞
【特許出願人】
【識別番号】　000003078
【住所又は居所】　神奈川県川崎市幸区堀川町７２番地
【氏名又は名称】　株式会社東芝
【代理人】　申請人
【識別番号】　100058479
【住所又は居所】　東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許法律事務所内
【氏名又は名称】　鈴江　武彦
【選任した代理人】
【識別番号】　100084618
【住所又は居所】　東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許法律事務所内
【氏名又は名称】　村松　貞男
【選任した代理人】
【識別番号】　100068814
【住所又は居所】　東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許法律事務所内
【氏名又は名称】　坪井　淳
【選任した代理人】
【識別番号】　100092196
【住所又は居所】　東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許法律事務所内
【氏名又は名称】　橋本　良郎
【選任した代理人】
【識別番号】　100091351
【住所又は居所】　東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許法律事務所内
【氏名又は名称】　河野　哲
【選任した代理人】
【識別番号】　100088683
【住所又は居所】　東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許法律事務所内
【氏名又は名称】　中村　誠
【選任した代理人】

【識別番号】　100070437
【住所又は居所】　東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許法律事務所内
【氏名又は名称】　河井　将次

出　願　人　履　歴　情　報

識別番号　　〔０００００３０７８〕

１．変更年月日　　１９９０年　８月２２日
［変更理由］　新規登録
住　所　神奈川県川崎市幸区堀川町７２番地
氏　名　株式会社東芝